REMARKS

The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Office Action dated November 10, 2004. In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due reconsideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Status of the Claims

As outlined above, claims 13 - 21 are currently pending in this application.

Other Amendments

The specification is being amended to correct various formal errors. Applicant hereby submits that no new matter is being introduced into the application through the submission of this response.

Prior Art Rejections

The Examiner rejected claims 13-21 under 35 U.S.C. § 102(e) as being anticipated by Hohle (U.S. Patent No. 6,199,762).

The present invention as recited in claim 13 is directed to a smart card system, comprising: a smart card issuance/management system configured to perform issuance and management of a smart card; and a smart card service providing/managing system configured to perform issuance and management of an application loaded on the smart card. The smart card issuance/management system and the smart card service providing/managing system are operatively connected to each other through a network such that information exchange is achieved by transmitting and receiving electronic messages through the network. Each of the electronic messages is uniquely identified using a message ID. Data of the smart card issuance/management system and the smart card service providing/managing system is stored using the message ID as a key. The information exchange between the smart card issuance/management system and the smart card service providing/managing system includes at the time of initial issuance of the smart card, the smart card issuance/management system sending an application loading permission which permits the smart card service providing/management system to load an application, at the time of reissuance of the smart card, the smart card issuance/management system searches the message ID of the application loading permission using card attribute data, which identifies the smart card and sends the message ID of the application loading permission, at the time of the initial issuance of the smart card, the smart card service providing/managing system sends the application loading permission and the application and loads the application in the smart card, and at the time of the reissuance of the smart card, the smart card service providing/managing system receives

the card attribute data from the smart card, sends the card attribute information and an application ID of the application to the smart card issuance/management system, and searches an examination result at the time of initial loading application using the message ID as the key.

According to new claim 16, the present invention is directed to a smart card issuance/management system configured to perform issuance and management of a smart card and configured to connect to a smart card service providing/managing system through a network, wherein information exchange is achieved by transmitting and receiving electronic messages through the network. Each of the electronic messages is uniquely identified using a message ID. Data of the smart card issuance/management system and the smart card service providing/managing system is stored using the message ID as a key. At the time of initial issuance of the smart card, the smart card issuance/management system sends an application loading permission which permits the smart card service providing/management system to load an application; and at the time of reissuance of the smart card, the smart card issuance/management system searches a message ID of the application loading permission using card attribute data, which identifies the smart card, as a key, and sends the message ID of the application loading permission.

Further, according to claim 19, the present invention is directed to a smart card service providing/managing system configured to perform issuance and management of a smart card and configured to connected to an IC card service issuance/management system configured to perform issuance and management an application loaded on the smart card, through the network, wherein information exchange is achieved by transmitting and receiving electronic messages through the network. Each of the electric messages is uniquely identified using a message ID. The data of the smart card issuance/management system and the smart card service providing/managing system is stored using the message ID as a key. At the time of initial issuance of the smart card, the smart card service providing/managing system receives an application loading permission from the smart card issuance/management system, which permits the smart card service providing/management system to load an application, and loads the application to the smart card; and at the time of reissuance of the smart card, the service providing/managing system receives the card attribute data from the smart card which identifies the smart card, sends the card attribute data and an application ID of the application, receives the message ID of the application loading permission, and searches an examination result at the time of initial loading application using the message ID as the key.

Support for the recitation of the newly submitted claims outlined above may be found on page 4, line 7 to page, 5 line 8, page 31, line 12 - page 36, line 11, and Fig. 8 (Claims 13, 16 and 19); page 12, line 11 - 13 (Claims 14, 17 and 20); and page 33, line 16 - 17 (Claims 15, 18, and 21).

key systems during the final phase of the smartcard issuance process (see column 2, lines 53 - 58). The method of Hohle allows key information to be securely downloaded to the smartcard without the intervention of a third party (column 10, lines 59 - 64).

Hohle does not disclose, teach or suggest a message ID that is used when exchanging the application loading permission. At best, the initialization data of Hohle may correspond to the message ID of the present invention. However, such data comprises only managed personal information when a card is issued, i.e. the "account number ....." in Hohle. Such data is quite different from the message ID of the present invention which is distinguished from other electronic messages uniquely (see page 34, lines 15-22).

In addition, Hohle especially does not disclose, teach or suggest any process or method wherein, at the time of initial issuance of the smart card, the smart card issuance/management system sending an application loading permission which permits the smart card service providing/management system to load an application, at the time of reissuance of the smart card, the smart card issuance/management system searches the message ID of the application loading permission using card attribute data, which identifies the smart card and sends the message ID of the application loading permission, at the time of the initial issuance of the smart card, the smart card service providing/managing system sends the application loading permission and the application and loads the application in the smart card, and at the time of the reissuance of the smart card, the smart card service providing/managing system receives the card attribute data from the smart card, sends the card attribute information and an application ID of the application to the smart card issuance/management system, and searches an examination result at the time of initial loading application using the message ID as the key.

At most, Hohle only shows an example of an issuer's construction and fails to show those of an issuer and a service provider. Therefore, Hohle cannot anticipate or render obvious the type of communication that is essential to and claimed for the present invention as the system of Hohle cannot embody that kind of communication between itself.

Consequently, Hohle does not and cannot disclose the procedure of reloading an application using the message ID that was used when exchanging the application loading permission. In particular, Hohle does not disclose, teach or suggest the characteristics of the invention as now recited in at least claims 13 and 19 wherein, "the data of the smart card issuance/management system and the smart card service providing/managing system is stored using the message ID as a key" and "the smart card service providing/managing system searches an examination result at the time of initial loading application using the message id as a key."

Further, Hohle does not disclose, teach or suggest the characteristics of the invention as now recited in claim 16 wherein "the data of the smart card issuance/management system and the smart card service providing/managing system is

Among the main features of the present invention, the smart card issuance/ management system (101) and the smart card service providing/managing system (107) store data using a message ID as a key. The "message ID" is an ID that uniquely identifies an electronic message used when exchanging the electronic message between the smart card issuance/management system and the smart card service providing/managing system. The smart card service providing/managing system searches an examination result at the time of initial loading application using the message ID that was used when exchanging the application loading permission, and then judges whether or not the application is reloadable.

For a smart card type system which does not permit third party access other than through a card, this system enables the smart card service providing/managing system to check whether or not an application that a user requests to be reloaded, was previously loaded in an old card, and then to judge whether or not the application is reloadable using an examination result at the time of initial application loading. Therefore, it is possible to simplify the reloading of an application to reduce the user's load at the time of reissuance, without having to rely on the procedure of initially loading of an application. Support for this invention is provided in the specification on page 4, line 6 to page 5 line 8; page 6, line 7 to page 7, line 16; page 11, line 16 to page 12, line 25; page 32, lines 3 - 8; page 36, lines 3 - 23; page 42, line 13 to page 43, line 2; and page 54, lines 7 - 15.

With respect to a specific embodiment of the present invention, as shown in Figure 8, when a service provider 121 and a card issuer 122 conduct exchanges required for service operation, the message ID is stored in each message. Figs 16 and 17 show examples of the data tables associated with such exchanges. Specifically, Fig. 16 shows an example of a data table relating to reissuing OK/NG that is stored in both the card issuer database and the service provider database. Fig. 17 shows an example of a data table related to the smart card, which is stored in the database by both of the card issuer and the service provider.

When an application reloading is requested, the card issuer transmits a "message ID" in an application loading permission to the service provider (step 807). The message ID is one used when the permission for loading the application, for which reloading is requested. At the next step, the service provider confirms the information according to this message ID, and can reload an application onto the smart card.

The present invention can reduce the amount of sending data in the communication system associated with a smart card system. Form the point of view of the card issuer, the data loads of the issuer can be reduced because the issuer can re-use the examination information from the initial loading of an application. One of the main advantages of the present invention is its simplicity.

In contrast to the present invention, the cited reference to Hohle is directed to the personalization of multi-function smartcards that is accomplished via a security server configured to generate and/or retrieve cryptographic key information from multiple enterprise

stored using the message ID as a key" and "the smart card issuance/management system sends the message ID of the application loading permission."

Consequently, the reference to Hohle fails to anticipate or render obvious each and every feature of the present invention as now claimed. Rather, the present invention as a whole is distinguishable and thereby allowable over the prior art.

Conclusion

In view of all the above, Applicant respectfully submits that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art upon which the rejection in the Office Action relies. These differences are more than sufficient that the present invention as now claimed would not have been anticipated nor rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

February 10, 2005
SPF/JCM